(12) UK Patent Application (19) GB (11) 2 384 406 (13) A

(43) Date of A Publication 23.07.2003

(21) Application No 0201282.1

(22) Date of Filing 21.01.2002

(71) Applicant(s)
Hyun Ku Yeun
43 Elizabeth Way, Mangotsfield, BRISTOL, BS16 9LN, United Kingdom

(72) Inventor(s)
Hyun Ku Yeun

(74) Agent and/or Address for Service
Withers & Rogers
Goldings House, 2 Hays Lane, LONDON, SE1 2HW, United Kingdom

(51) INT CL[7]
H04L 9/08 29/06

(52) UK CL (Edition V)
H4P PDCSA PDCSP

(56) Documents Cited
EP 0816970 A2
WO 2001/082036 A2
US 6076163 A

(58) Field of Search
UK CL (Edition T) H4P PDCSA PDCSC PDCSP PPEB
INT CL[7] G06F 1/00, H04L 9/08 9/30 9/32 29/06
Other: ONLINE DATABASES: WPI, EPODOC, JAPIO.

(54) Abstract Title

Three party cryptosystem having pairs of private keys

(57) Users (A, B) of a cryptosystem send and receive messages with the help of a trusted third party (TTP) using private keys (X) and public keys (P) which encapsulate said private keys. Each user (A, B) holds a private key (X_{A1}, X_{B1}) and the third party is entrusted with a corresponding private key (X_{A2}, X_{B2}) for each user. The trusted third party responds to a challenge (CHA) from a user by issuing a response (RES) which encapsulates the corresponding private key (X_{A2}, X_{B2}) so that the user can use the response in combination with the private key (X_{A1}, X_{B1}) it already holds to decrypt or sign a message. The response takes the form $r_2^{HX_{B1}} \bmod p$, where r is a private parameter, p is a public system parameter (eg. a large prime) and H is an exponent function (eg. a one-way, collision-resistance hash function). The message (e) is then decrypted to obtain the original message (m) via $m = e\,(r_1^{HX_{B1}}\,RES)^{-1} \bmod p$.

This system removes the need for key escrow or Public Key Infrastructure (PKI) since the trusted third party is required to know only a private key corresponding to the private key of each user, rather than the user's private key itself.

GB 2 384 406 A

CRYPTOSYSTEM

This invention relates to cryptosystems and methods for encrypting/decrypting and signing messages.

In 1976 Diffie and Hellman introduced the public key exchange that is based on the Diffie Hellman Problem (DHP) that is closely related to the well known Discrete Logarithm Problem (DLP). The intractability of DLP is equivalent to the security of the ElGamal public key scheme. The RSA public key cryptosystem was introduced in 1978, and may be used for both secrecy and digital signatures. The RSA cryptosystem works in Z_n, where n is the product of two large primes p and q, and its security is based on the difficulty of factoring n, that is, the integer factorization problem. Since then, various ElGamal and RSA type cryptosystems have been proposed to enhance existing defences against "chosen ciphertext attacks".

In 1984 Shamir proposed identity-based cryptosystems and signature schemes that enable simple key management in email systems. For example, when Alice sends an email to Bob at bob@cipherdoctor.com, she simply encrypts her message using the public key string bob@cipherdoctor.com. There is no need for Alice to obtain Bob's public key certificate. When Bob receives the encrypted email he contacts a Trusted Third Party (TTP). Bob authenticates himself to the TTP and obtains his private key from the TTP. Bob can then read his email. This system does not require a Public Key Infrastructure (PKI) so Alice can send encrypted email to Bob even if Bob has not set up his public key certificate. However, this system employs key escrow since the TTP knows Bob's private key.

An object of the invention is to provide an improved cryptosystem which has equivalent functionality to ID based public key cryptosystems, but which avoids the need for key escrow/PKI.

The invention consists in a cryptosystem in which users send and receive messages with the help of a trusted third party for security purposes making use of private keys and public parameters which encapsulate said private keys, each user holding a private key and the

trusted third party being entrusted with a corresponding private key for each user, and the trusted third party being adapted so that it is responsive to a challenge from a user by issuing a response which encapsulates the corresponding private key so that the user can use the response in combination with the private key already held by the user to decrypt or sign a message.

When the cryptosystem operates to encrypt/decrypt a message, the transmitting user encrypts the message to a recipient user using the public parameters which encapsulate the private keys of the recipient user. One of these private keys is held by the recipient user, but the other is held by the trusted third party, and thus the recipient user issues a challenge to the trusted third party so as to obtain a response in which the other private key is encapsulated. The private key held by the trusted third party is therefore kept secret, but it can be accessed by the recipient in its encapsulated form and used to decrypt the message.

Preferably, the encryption process also makes use of private parameters generated by the transmitting user, and these are transmitted to the recipient user for use in the challenge and response so that the decryption process is suitably enabled. These private parameters, as well as increasing encryption security, also serve to encapsulate the private key in the response.

When the cryptosystem operates to sign a message, the transmitting user creates a multi-part signature which is transmitted with the message so that a recipient user can check the signature against the signed message. The signature comprises one part generated directly by the transmitting user so as to encapsulate the private key held by the transmitting user, and another part encapsulating the response from the trusted third party following a challenge by the transmitting user, so that it incorporates the private key of the transmitting user held in trust by the trusted third party.

Preferably, the signature also includes a private parameter generated by the transmitting user which is used in generating the other two parts of the signature and which is transmitted with said other two parts to the recipient user for checking the signed message. This serves to increase signature security.

The challenge preferably makes use of the ID of the user issuing the challenge, and this ID is also incorporated in the encryption process or signing process. However, it is a feature of the invention that, although the encryption and signing processes involve private keys, the challenge does not use a private key and thus the private keys held by users are kept secret from the trusted third party.

The invention will now be described by way of example with reference to encryption and decryption of a message, and signing a message.

A trusted third party or key center TTP is established and publishes the public system parameters required by users of the cryptosystem to encrypt and sign messages. The cryptosystem is based on the Diffie-Hellman scheme over multiplicative group Zp, which is cyclic. The public system parameters consist of:

p - a large prime,
q - a large prime divisor of p - 1,
g_1 and g_2 - integers of order q where ($1 < g_1, g_2 < q$),
h - a one-way collision-resistance hash-function.

Also, each user has two private keys X, one being held by and being secret to the user, and the other being held by and being secret to the TTP. For example, a typical user Alice has a private key X_{A_1}, and the TTP holds a corresponding private X_{A_2}, where ($1 < X_{A_1}, X_{A_2} < q$); and a typical user Bob has a private key X_{B_1}, and the TTP holds a corresponding private key X_{A_2}, where ($1 < X_{B_1}, X_{B_2} < q$).

Based on these private keys $X_{A_1}, X_{A_2}, X_{B_1}, X_{B_2}$ corresponding public parameters P are published as follows:

$$P_{A_1} = g_1^{X_{A_1}} \bmod p$$
$$P_{A_2} = g_2^{X_{A_2}} \bmod p$$
$$P_{B_1} = g_1^{X_{B_1}} \bmod p$$
$$P_{B_2} = g_2^{X_{B_2}} \bmod p$$

Thus the public system parameters consist of p, q, h, g_1, g_2, P_{i1},P_{i2},where i = A, B, ...l.

In order to encrypt a message m ∈ Z_p, a user, such as Alice who wants to send a message to Bob, randomly chooses two integers k_1 and k_2, where 1 <k_1, k_2 <q, and computes the following:

$$r_1 = g_1^{k_1} \bmod p,$$
$$r_2 = g_2^{k_2} \bmod p,$$
and $$H = h(r_1, r_2 ID),$$

where ID is the binary string for the email address of Bob, for example, bob@cipherdoctor.com. The encrypted message e is then generated as follows:

$$e = mP_{B_1}^{Hk_1} P_{B_2}^{Hk_2} \bmod p.$$

Alice sends the encrypted message e and the parameters r_1 and r_2 to Bob.

In order to decrypt the encrypted message e, Bob first computes CHA = (r_1, r_2, ID) and sends this as a challenge to TTP. TTP then computes H = h(CHA) = h(r_1, r_2, ID) and sends Bob a response RES = $r_2^{HX_{B_2}} \bmod p$.

Bob then uses the response RES together with his private key X_{B_1} to decrypt the message as follows:

$$m = e(r_1^{HX_{B_1}} RES)^{-1} \bmod p.$$

It can be shown by simple substitution that this decryption formulation for m is the inverse function of the encryption formulation of e quoted above, and thus decryption is effective.

In order to sign a message m ∈ Z_p, Alice randomly chooses two integers k_1 and k_2, where 1 <k_1, k_2 <q, and computes the following:

$$r = mg_1^{k_1} g_2^{k_2} \bmod p,$$
$$H = h(r, m, ID),$$
and $$s_1 = k_1 - HX_{A_1} \bmod q.$$

Alice then computes CHA = (r, m, ID) and sends this as a challenge to TTP.

TTP then computes H = h(CHA) and sends Alice a response RES = $g_2^{-HX_{A_2}}$.

Alice then computes

$$s_2 = g_2^{k_2} RES \bmod q = g_2^{k_2 - HX_{A_2}} \bmod q.$$

Alice then sends Bob a signature message Sig(m) = (r, s_1, s_2) which Bob can use to verify the message m by substitution in the formulation:

$$r = mg_1^{s_1} s_2 P_{A_1}^H P_{A_2}^H \bmod p.$$

Thus if the signatory follows the above signature protocol, the recipient can be certain as to the true identity of the signatory.

In order to add message recovery to a digital signature scheme, a public redundancy function R and its inverse R^{-1} are introduced, the selection of R being critical to the security of the system.

To sign a message m $\in Z_p$, Alice randomly chooses two integers k_1 and k_2, where $1 < k_1, k_2 < q$, and computes the following:

$$m' = R(m),$$
$$r = m' g_1^{-k_1} g_2^{-k_2} \bmod p,$$
$$H = h(r, ID),$$
and $$s_1 = k_1 - HX_{A_1} \bmod q.$$

Alice then computes a challenge CHA = (r, ID) and sends it to TTP. TTP then computes H = h(CHA) and sends the response RES = $g_2^{-HX_{A_2}}$ to Alice. Alice then computes:

$$s_2 = g_2^{k_2} RES \bmod q = g_2^{k_2 - HX_{A_2}} \bmod q.$$

Alice then sends the signature message Sig(m) = (r, s_1, s_2) to Bob. After receiving Sig(m), the message is verified by Bob using the formulation:

$$m' = r g_1^{s_1} s_2 P_{A_1}^H P_{A_2}^H \bmod p.$$

After checking the validity of m', the message is recovered by computing

$$m = R^{-1}(m').$$

Whilst the invention has been described above with reference to a cryptosystem having just one trusted third party TTP, it will be appreciated that two or more TTPs may be provided, each being entrusted with a corresponding unique private key X_{a_n} for each user, so that a user is required to perform a challenge and response routine with each TTP before the user has all of the encapsulated private keys required for decrypting or signing a message.

Also, whilst the pairs of public parameters P_{A_1}, P_{A_2} and P_{B_1}, P_{B_2} involve system parameters g_1 and g_2, which take different values, g_1 and g_2 could be set at the same value to simplify the system. Also, where there are two or more TTPs, the values of two or more of the system parameters g_1, g_2, ... g_n could be the same.

The security of the proposed scheme is based on the security of Diffie-Hellman problem and one-way collision resistance hash-functions. Given the fact that there is no known method for "breaking" DHP or for finding collisions on one-way collision-resistance hash-functions, it is computationally infeasible to break the proposed scheme.

It will be appreciated that the use of two or more private keys per user, one held by the user and one by each TTP, and the challenge and response technique with each TTP, enables a

computationally secure cryptosystem to be set up without embedding key escrow and without any PKI requirement so all users enjoy secure communication with each other without possessing verified certificates. The invention therefore provides an implicitly authenticated public key cryptosystem which avoids disclosing user's private keys even to the TTP.

CLAIMS

1. A cryptosystem in which users (A, B) send and receive messages (m) with the help of a trusted third party (TTP) for security purposes making use of private keys (X) and public parameters (P) which encapsulate said private keys (X), each user (A, B) holding a private key (X_{A_1}, X_{B_1}) and the trusted third party (TTP) being entrusted with a corresponding private key (X_{A_2}, X_{B_2}) for each user (A, B), and the trusted third party (TTP) being adapted so that it is responsive to a challenge (CHA) from a user (A, B) by issuing a response (RES) which encapsulates the corresponding private key (X_{A_2}, X_{B_2}) so that the user (A, B) can use the response (RES) in combination with the private key (X_{A_1}, X_{B_1}) already held by the user (A, B) to decrypt or sign a message.

2. A cryptosystem as claimed in claim 1 in which users (A, B) generate private parameters (r; r_1, r_2) which encapsulate user parameter selections (k_1, k_2) and which are incorporated in the challenge (CHA) and response (RES).

3. A cryptosystem as claimed in claim 2 in which a transmitting user (A) encrypts a message (m) to a recipient user (B) using the public parameters (P_{B_1}, P_{B_2}) which encapsulate the private keys (X_{B_1}, X_{B_2}) of that recipient user (B), and private parameters (r_1, r_2) generated by the transmitting user (A), the private parameters (r_1, r_2) being transmitted to the recipient user (B) to decrypt the encrypted message (e).

4. A cryptosystem as claimed in claim 3 in which the transmitting user (A) selects integers (k_1, k_2) and uses each in a public generator function to generate a respective private parameter (r_1, r_2).

5. A cryptosystem as claimed in claim 4 in which the message (m) is encrypted according to the general formulation

$$mP_{B_1}^{Hk1}P_{B_2}^{Hk2} \bmod p,$$

where H is an exponent function that incorporates the private parameters (r_1, r_2) and p is a

public system parameter in the form of a large prime integer.

6. A cryptosystem as claimed in claim 5 in which the public generator function for the private parameters (r_1, r_2) takes the form

$$r_1 = g_1^{k1} \bmod p$$

and $r_2 = g_2^{k2} \bmod p$,

and in which $P_{B_2} = g_1^{X_{B_1}} \bmod p$

and $P_{B_2} = g_2^{X_{B_2}} \bmod p$,

where g_1 and g_2 are public system parameters.

7. A cryptosystem as claimed in claim 6 in which $g_1 = g_2$.

8. A cryptosystem as claimed in any one of claims 5 to 7 in which the exponent function H incorporates the identity (ID) of the transmitting user (A).

9. A cryptosystem as claimed in any one of claims 5 to 8 in which the exponent function H comprises a one-way, collision-resistance hash function (h).

10. A cryptosystem as claimed in any one of claims 5 to 8 in which the response RES takes the general form

$$r_2^{HX_{B_2}} \bmod p.$$

11. A cryptosystem as claimed in claim 10 in which the recipient user (B) decrypts the encrypted message (e) to recover the original message (m) using the formulation

$$m = e\,(r_1^{HX_{B_1}} RES)^{-1} \bmod p.$$

12. A cryptosystem as claimed in any one of the preceding claims in which the challenge (CHA) incorporates the identity (ID) of the recipient user (B).

13. A cryptosystem as claimed in claim 2 in which a transmitting user (A) signs a message (m) by creating a multi-part signature message Sig(m) which is transmitted with the message (m) so that a recipient user (B) can check the signature message Sig(m) against the message (m), the signature message comprising one part (s_1) generated directly by the user (A) so as to encapsulate the user's private key (X_{A_1}), and another part (s_2) encapsulating the response (RES) from the trusted third party (TTP).

14. A cryptosystem as claimed in claim 13 in which the multi-part signature message Sig(m) includes the private parameter (r).

15. A cryptosystem as claimed in claim 14 in which the private parameter (r) is generated by a public generator function that takes the general form

$$r = mg_1^{k_1} g_2^{k_2} \bmod p$$

where g_1, g_2 and p are public system parameters and p is a large prime integer.

16. A cryptosystem as claimed in claim 15 in which $g_1 = g_2$.

17. A cryptosystem as claimed in any one of claims 13 to 16 in which the challenge (CHA) incorporates the private parameter (r), the identity (ID) of the transmitting user (A) and the message (m).

18. A cryptosystem as claimed in claim 14 or 16 in which the response (RES) takes the form

$$g_2^{-HX_{A_2}}$$

where H is an exponent function that incorporates the private parameter (r), the identity (ID) of the transmitting user (A) and the message (m).

19. A cryptosystem as claimed in claim 18 in which the exponent function H is a one-way, collision-resistance hash function (h).

20. A cryptosystem as claimed in any one of claims 13 to 19 in which the parts (s_1, s_2) of the signature message Sig(m) take the general form

$$s_1 = k_1 - HX_{A_1} \bmod q$$

and $$s_2 = g_2^{-k_2} RES \bmod q$$

where q is a public system parameter in the form of a large prime division of p-1.

21. A cryptosystem as claimed in any one of the preceding claims which involves two or more trusted third parties (TTP), each of which is entrusted with a corresponding private key ($X_{a_2}, X_{b_2}; X_{a_3}, X_{b_3}$) for each user (A, B), each being adapted to respond to a challenge (CHA) from a user (A, B) by issuing a response (RES) which encapsulates the corresponding private key ($X_{a_2}, X_{b_2}; X_{a_3}, X_{b_3}$).

22. A cryptosystem as claimed in claim 7 or 16 which involves two or more trusted third parties (TTP), each of which is entrusted with a corresponding private key (X) for each user (A, B), each being adapted to respond to a challenge (CHA) from a user (A, B) by issuing a response (RES) which encapsulates the corresponding private key (X), and the values of two or more of the system parameters (g_n) are the same.

23. A cryptosystem for encrypting messages to be transmitted from a transmitting user (A) to a recipient user (B) and for decrypting received messages with the help of a trusted third-party (TTP), the system making use of at least two private keys for each user, one private key (X_{B_1}) being held by the user and the other private key (X_{B_2}) being held by the trusted third-party (TTP), each message (m) being encrypted by the transmitting user (A) in accordance with public user parameters (P_{B_1}, P_{B_2}) that incorporate the private keys (X_{B_1}, X_{B_2}) of an intended recipient user (B) so that said recipient user (B) can only decrypt the message after a challenge (CHA) to the trusted third party (TTP) and a response (RES)

from the trusted third party (TTP) in which the said other private key (X_{B_2}) is encapsulated.

24. A signature system for authenticating a message as originating from a user (A) by the user (A) encrypting the message (m) using one or more user encryption parameters (k_1, k_2) selected by the user (A), and using said user encryption parameters (k_1, k_2) to generate encapsulated signed messages (s_1, s_2) which are transmitted with the encrypted message (r) to a user (B) to allow authentication of the encrypted message (r) by the user (B) successfully decrypting it, the encapsulated signed messages (s_1, s_2) each incorporating a private key, one private key (X_{A_1}) being held by the user (A) and the other private key (X_{A_2}) being held by a trusted third-party (TTP) and only being released by the trusted third-party (TTP) in an encapsulated form (RES) when it receives a challenge (CHA) from the user (A).

PPK/D

13

INVESTOR IN PEOPLE

Application No: GB 0201282.1 **Examiner:** Mark Lewney
Claims searched: All **Date of search:** 29 August 2002

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.T): H4P (PDCSA, PDCSC, PDCSP, PPEB)

Int Cl (Ed.7): G06F (1/00), H04L (9/08, 9/30, 9/32, 29/06)

Other: Online databases: WPI, EPODOC, JAPIO.

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
A	EP0816970A2	(SUN MICROSYSTEMS) - Consider whole document.	
A	WO01/82036A2	(NETCERTAINTY INC.) - See especially lines 14-18 on p. 5.	
A	US6076163	(HOFFSTEIN ET AL.) - See especially lines 39-58, col 7 and figure 3.	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.